



# PROJET VERGIS CORPORATION-Conception Reseau

CHOIX DE SPECIFICATIONS

*Groupe 2*

AKAWI TOUMBAROU – DJIOJIP CLAUDE - KWAMOU AXELLE - NDOUMBE RALPH

## TABLE DE MATIERES

<b>INTRODUCTION.....</b>	<b>2</b>
<b>PLAN D'ADRESSAGE ET VLAns.....</b>	<b>3</b>
<i>1. Choix des classes d'adresses et Élaboration du plan d'adressage .....</i>	<i>3</i>
<b>REDONDANCE .....</b>	<b>7</b>
- <b>ETUDE COMPARATIVE DES PROTOCOLES .....</b>	<b>7</b>
<b>PROTOCOLE DE ROUTAGE DYNAMIQUE (EIGRP ET OSPF).....</b>	<b>9</b>
- <b>ETUDE COMPARATIVE DES PROTOCOLES .....</b>	<b>9</b>
<b>PROTOCOLE DE SECURITE (PAREFEU) .....</b>	<b>11</b>
<b>CHOIX des équipements .....</b>	<b>13</b>

## INTRODUCTION

Après l'attaque de leur entreprise, Vergis Corporation, désire améliorer l'architecture du réseau de l'entreprise ainsi que sa sécurité. Pour ce faire, ils font appel à notre équipe afin de mener à bien cette tâche.

Pour un souci de transparence et de traçabilité de notre travail, nous allons dans ce document, présenter et justifier les choix retenus pour notre architecture réseau. Ainsi, nous présenterons :

- **PLAN D'ADRESSAGE & VLANs**
- **PROTOCOLE DE REDONDANCE CHOISI**
- **PROTOCOLES DE ROUTAGE**
- **PROTOCOLES DE SECURITE (PAREFEU)**

## PLAN D'ADRESSAGE ET VLANS

Pour commencer, nous avons réparti les différents services en Vlan et évaluer le nombre de machines dont nous aurions besoin afin de ressortir un plan d'adressage adéquat.

**Les vlans du site principal repartis dans ce tableau :**

Numero de VLANs	Noms de services	Nombre d'hôtes /services
15	<i>Informatique -Support</i>	6
2	<i>Logistique</i>	8
3	<i>Comptabilité</i>	4
4	<i>Secrétariat</i>	14
5	<i>Recherche &amp; développement</i>	144
6	<i>Direction</i>	10
7	<i>Ressources Humaines (RH)</i>	4
8	<i>Secrétariat de direction</i>	4
9	<i>Communication</i>	8
10	<i>Support Client</i>	25
11	<i>Informatique -Développement</i>	10
12	<i>Informatique -Infrastructure</i>	4
13	<i>Commerciaux</i>	5
14	<i>Administration</i>	5

### **DATACENTER : 172.17.2.160/28**

- Serveur FTP : **172.17.2.170**
- Serveur WEB : **172.17.2.169**, Gateway : **172.17.2.162**;
- Serveur DNS: **172.17.2.174**;
- Serveur RH : **172.17.2.167**, Gateway : **172.17.2.162**
- Serveur Intranet :**172.13.2.170**, Gateway : **172.13.2.172**
- Serveur SMTP : **172.17.2.168**

### **1. Choix des classes d'adresses et Élaboration du plan d'adressage**

De nos études, nous avons appris que les adresses de classes **C** avait un nombre limite de 254 hôtes par réseau, or pour le réseau du site principal nous avons un service à lui seul qui prend un ensemble de 254 hôtes, d'où effectuer un adressage avec les adresses de type C sera préjudice.

De ce fait nous avons décidé de travailler avec des adresses de classes **B** particulièrement pour leur capacité à prendre en charge **65000 hôtes /réseau**, ce qui est largement suffisant pour couvrir, non seulement l'adressage du site principal mais également, pour celui de la datacenter, site secondaire et de l'agence.

Par ailleurs, nous avons utilisé la méthode **VSLM (Variable Length Subnet Mask)** : car nous avons à faire ici, a **un ensemble de sous-réseau (VLANs)** et notre objectif est **de limiter le gaspillage d'adresses**

**Bloc d'adresses : 172.18.0.0/16 ;**

L'attributions des pools d'adresses se font dans le tableau ci-dessous :

- **SITE PRINCIPAL**

<i>Numero de VLANs</i>	<i>Adresses de réseau</i>	<i>Pool d'adresses</i>	<i>Adresses de diffusion</i>	<i>Masque de sous réseau</i>	<i>Nombre d'hôtes</i>
<b>5</b>	172.18.1.0	<b>172.18.1.1-172.18.1.254</b>	172.18.1.254	255.255.255.0/24	144
<b>10</b>	172.18.2.0	<b>172.18.2.1-172.18.2.30</b>	172.18.2.31	255.255.255.224/27	25
<b>4</b>	172.18.2.32	<b>172.18.2.33-172.18.2.46</b>	172.18.2.47	255.255.255.240/28	14
<b>6</b>	172.18.2.48	<b>172.18.2.49-172.18.2.62</b>	172.18.2.63	255.255.255.240/28	10
<b>11</b>	172.18.2.64	<b>172.18.2.65-172.18.2.78</b>	172.18.2.79	255.255.255.240/28	10
<b>2</b>	172.18.2.80	<b>172.18.2.81-172.18.2.94</b>	172.18.2.95	255.255.255.240/28	8
<b>9</b>	172.18.2.96	<b>172.18.2.97-172.18.2.110</b>	172.18.2.111	255.255.255.240/28	8
<b>15</b>	172.18.2.112	<b>172.18.2.113-172.18.2.118</b>	172.18.2.119	255.255.255.248/29	6
<b>13</b>	172.18.2.120	<b>172.18.2.121-172.18.2.126</b>	172.18.2.127	255.255.255.248/29	5

<b>3</b>	172.18.2.128	<b>172.18.2.129-172.18.2.134</b>	172.18.2.135	255.255.255.248/29	4
<b>7</b>	172.18.2.136	<b>172.18.2.137-172.18.2.142</b>	172.18.2.143	255.255.255.248/29	4
<b>8</b>	172.18.2.144	<b>172.18.2.145-172.18.2.150</b>	172.18.2.151	255.255.255.248/29	4
<b>12</b>	172.18.2.152	<b>172.18.2.153-172.18.2.158</b>	172.18.2.159	255.255.255.248/29	4
<b>Administration</b>	172.18.2.160	<b>172.18.2.161-172.18.2.166</b>	172.18.2.167	255.255.255.248/29	5

L'adressage des routeurs est établi sur le reseau de caracteristiques ;

- Adresse de reseau : **172.18.3.0/16** ;
- Masque de sous-réseau : **255.255.255.240/28** ;
- Pool d'adresses : **172.18.3.1 – 172.18.3.14** ;
- Adresses de diffusion : **172.18.3.15** ;

- **SITE SECONDAIRE**

<i>Numero de VLANs</i>	<i>Adresses de reseau</i>	<i>Pool d'adresses</i>	<i>Adresses de diffusion</i>	<i>Masque de sous reseau</i>	<i>Nombre d'hôtes</i>
<b>5</b>	172.18.3.0	<b>172.18.3.1-172.18.3.254</b>	172.18.3.255	255.255.255.0/24	144
<b>10</b>	172.18.4.0	<b>172.18.4.1-172.18.4.30</b>	172.18.4.31	255.255.255.224/27	25
<b>4</b>	172.18.4.32	<b>172.18.4.33-172.18.4.46</b>	172.18.4.47	255.255.255.240/28	14
<b>6</b>	172.18.4.48	<b>172.18.4.49-172.18.4.62</b>	172.18.4.63	255.255.255.240/28	10
<b>11</b>	172.18.4.64	<b>172.18.4.65-172.18.4.78</b>	172.18.4.79	255.255.255.240/28	10
<b>2</b>	172.18.4.80	<b>172.18.4.81-172.18.4.94</b>	172.18.4.95	255.255.255.240/28	8

<b>9</b>	172.18.4.96	<b>172.18.4.97- 172.18.4.110</b>	172.18.4.111	255.255.255.240/28	8
<b>15</b>	172.18.4.112	<b>172.18.4.113- 172.18.4.118</b>	172.18.4.119	255.255.255.248/29	6
<b>13</b>	172.18.4.120	<b>172.18.4.121- 172.18.4.126</b>	172.18.4.127	255.255.255.248/29	5
<b>3</b>	172.18.4.128	<b>172.18.4.129- 172.18.4.134</b>	172.18.4.135	255.255.255.248/29	4
<b>7</b>	172.18.4.136	<b>172.18.4.137- 172.18.4.142</b>	172.218.4.143	255.255.255.248/29	4
<b>8</b>	172.18.4.144	<b>172.18.4.145- 172.18.4.150</b>	172.18.4.151	255.255.255.248/29	4
<b>12</b>	172.18.4.152	<b>172.18.4.153- 172.18.4.158</b>	172.18.4.159	255.255.255.248/29	4
<b>Administration</b>	172.18.4.160	<b>172.18.4.161- 172.18.4.166</b>	172.18.4.167	255.255.255.248/29	5

- **DATACENTER**

Étant donné que le datacenter est cet emplacement qui contient que des serveurs et des backups du site, nous avons alloué une plage d'adresse qui sera administrée de façon statique ;

- Adresse de réseau : **172.17.2.168**
- Masque de sous-réseau : **255.255.255.240/28;**
- Pool d'adresses : **172.17.2.161 - 172.17.2.174;**
- Adresses de diffusion : **172.17.2.175;**

## REDONDANCE

### - ETUDE COMPARATIVE DES PROTOCOLES

<i>Base de comparaison</i>	<i>HSRP</i>	<i>VRRP</i>	<i>GLBP</i>
<i>Un routeur configure comme actif</i>	Oui	Oui	Oui (plusieurs routeurs peuvent être déclaré comme actif)
<i>Propriétaire Cisco</i>	Oui	Non (open standard)	Oui
<i>Plus deux routeurs dans un groupe</i>	Oui	Oui	Oui
<i>Prends en charge le suivi</i>	Oui	Oui	Oui
<i>Prends en charge IPv4 et IPv6</i>	Oui	Oui mais uniquement le VRRPv3	Oui
<i>Rapidité</i>	Moins rapide	Rapide mais consomme la mémoire	Moins rapide mais optimal
<i>Authenticité</i>	Oui	Non (supporter sur cisco)	Oui
<i>Temps par Défaut</i>	Hello : 3 secondes Temps d'attente : 10 secondes	Hello : 1 secondes Temps d'attente : 3 secondes	Hello : 3 secondes Temps d'attente : 10 secondes
<i>Implémentation</i>	Facile	Facile	Modéré
<i>IP Virtuel et MAC</i>	Un IP virtuel et une MAC virtuel	Un IP virtuel ou IP réel du routeur et une MAC virtuel	Une IP virtuelle, plusieurs MAC virtuel
<i>Équilibrage de charge du trafic</i>	Non	Non	Oui

**Conclusion :** Selon le tableau de comparaison ci-dessus, nous avons choisi **le protocole GLBP** à cause de la raison suivante :



- Il permet **de faire l'équilibrage de charge du trafic** et donc **réduira la latence du réseau lors d'une surcharge**.
- Et au niveau **de la rapidité** il est **moins rapide que le VRRP** mais pas si que ça puisque'il **n'utilise pas beaucoup de mémoire** et donc **pourra à la longue démontrer son efficacité**.

## PROTOCOLE DE ROUTAGE DYNAMIQUE (EIGRP ET OSPF)

### - ETUDE COMPARATIVE DES PROTOCOLES

Base de comparaison	EIGRP	OSPF
<b>Signifie</b>	Protocole de passerelle intérieure amélioré	Ouvrez le chemin le plus court en premier
<b>Basé sur des normes</b>	Propriété de Cisco	Norme ouverte IETF industriel standard ouvert
<b>Type de protocole</b>	Hybride	État du lien
<b>Métriques de routage</b>	Combinaison de bande passante, fiabilité, charge et délai.	Bande passante d'interface
<b>Distance administrative</b>	90 (interne) 170 (externe)	110
<b>Exigences du processeur</b>	Besoins en CPU et mémoire réduits	Nécessite un processeur et une mémoire élevés
<b>Algorithme</b>	Vecteur de distance DUAL	État du lien Dijkstra
<b>Conception hiérarchique</b>	Non	Oui
<b>Prise en charge d'IPX et d'AppleTalk</b>	Oui	Non
<b>Mises à jour</b>	Mises à jour et requêtes selon les besoins vers une adresse multicast	Inondation au besoin et périodiquement vers une adresse multicast
<b>Facilité de mise en œuvre</b>	Facile mais pas de fourniture de résumé automatique	Complicé
<b>Prévention des boucles</b>	Horizon partagé et DUAL	Connaissance complète de la topologie
<b>Filtrage et synthèse</b>	Possible n'importe où dans le réseau	Uniquement sur les ASBR ou ABR
<b>Vitesse de convergence</b>	Très rapide	Rapide

<b>Relation voisine</b>	Simple	Complexe

### **Conclusion :**

Notre choix se porte sur **le protocole EIGRP** parce qu' :

- Il est **protocole Cisco** et nous allons travailler sur **le logiciel de simulation Cisco Packet tracer**.
- Il utilise **un protocole hybride** c'est à dire ; **vecteur à distance et état de liens**.
- **Le filtrage et la synthèse qui se fait n'importe où dans le réseau**.
- Ce protocole **ne nécessite pas assez de mémoire**.

## PROTOCOLE DE SECURITE (PAREFEU)

### - ETUDE COMPARATIVE DES PROTOCOLES DE SECURITE PAREFEU

Ils ont été recensés dans ce tableau

	UTM/NGFW	Routeur filtrant	Pf sense
<b>Services proposes</b>	<ul style="list-style-type: none"> <li>- NAT, VPN</li> <li>- Filtrage d'URL, IP, Protocoles</li> <li>- Restriction de mise a jour de routage</li> <li>- Contrôles d'applications</li> <li>- Pas de fichiers logs</li> <li>- Service d'acheminement a distance</li> </ul>	<ul style="list-style-type: none"> <li>- Filtrages IP, protocoles</li> <li>- Restrictions de mise à jour</li> <li>- Pas de fichiers logs</li> </ul>	<ul style="list-style-type: none"> <li>- NAT</li> <li>- Filtrage IP et protocoles</li> <li>- Présence de fichiers logs</li> <li>- VPN Open source</li> <li>- Prévention d'intrusions Ips / Ids</li> </ul>
<b>Administration</b>	<ul style="list-style-type: none"> <li>- A l'aide d'une interface WEB</li> <li>- Configuration centralisée</li> <li>- Prise en main complexe</li> </ul>	<ul style="list-style-type: none"> <li>- Configuration graphique (GUI)</li> <li>- Procédure : longue</li> <li>- La syntaxe d'ACL est spécifique à chaque routeur</li> <li>- Prise en main moyenne</li> <li>- Sur console (CLI)</li> </ul>	<ul style="list-style-type: none"> <li>- A l'aide d'une interface WEB</li> <li>- Prise en main facile</li> </ul>
<b>Cout</b>	Coût élevé	Coût moyen	Open source

				Gratuit (License)
Sécurité	Type	Périmétrique	Périmétrique	Périmétrique
	Niveau	Maximale	Optimale	Optimale
Domaines d'applications		<ul style="list-style-type: none"> <li>- Multinationales</li> <li>- FAI</li> <li>- Banques</li> </ul>	PME + domaines UTM / NFWG	PME / PMI uniquement
Implémentation		<ul style="list-style-type: none"> <li>- Facile</li> <li>- Ne requiert qu'un seul équipement</li> </ul>	Équipements (routeur)	Équipements (machine)

### **Conclusion :**

Au vu de la nature de l'entreprise vergis, nous avons opté pour une sécurisation à l'aide de pare-feu **NGFW** suivi de configurations **ACL** pour plus de sécurités

## CHOIX DES EQUIPEMENTS

Nous avons :

- **Switch de niveau 3** : nous avons choisi le switch de niveau 3 au détriment du switch de niveau 2 et routeur car en termes de **cout**, le switch de niveau 3 est **MOINS COUTEUX qu'un routeur**. De plus, le switch de niveau 3 est **plus performant** que le switch de niveau 2 car il intègre les fonctions de **routage** assimilable à celui d'un routeur.

Un switch de niveau 2 fonctionne uniquement avec les adresses **MAC** et ne fait pas attention aux **adresses IP** ou à **tout autre élément des couches supérieures**. Un switch de niveau 3, ou **switch multicouche**, peut effectuer toutes les tâches d'un switch de niveau 2. Le switch de niveau 3 peut également effectuer un **routage statique** et un **routage dynamique**. Cela signifie qu'il dispose à la fois d'une table d'adresses MAC et d'une table de routage IP, et gère la communication intra-VLAN ainsi que le routage de paquets entre différents VLAN

**Nb : toutefois, ce switch n'est utilisé que si nécessaire**